UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/468,377	12/20/1999	YURIJ ANDRIJ BARANSKY	Y0999-558	3573

7590 02/20/2004

DOUGLAS W CAMERON
INTELLECTUAL PROPERTY LAW DEPT
IBM CORPORATION P O BOX 218
YORKTOWN HEIGHTS, NY 10598

EXAMINER	
NALVEN, ANDREW L	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 02/20/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/468,377	BARANSKY ET AL.	
	Examiner	Art Unit	
	Andrew L Nalven	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 December 2003*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 December 1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-17 are pending.

Response to Arguments

2. Applicant's arguments filed 11 December 2003 have been fully considered but they are not persuasive.

3. Applicant has stated on Page 11 of amendment that the present invention distinguishes itself from the Thomlinson patent (US Patent No 6,389,535) because the present invention expressly omits the service provider from encryption and authentication processes. Examiner contends the claimed limitations only show the steps involved between a content provider and a user in establishing encryption and authentication processes. The Thomlinson reference does teach only two entities (user and provider) involved with establishing encryption and authentication processes.

4. Applicant further states that the Thomlinson patent teaches keys that are reversed from what is claimed by the present invention. The present invention claims two keys, a first key known only to the service provider and a second key that is encrypted using the first key and a one-time password and is then stored on the client machine. The second key is then used to access data. Examiner contends that the Thomlinson patent does teach a first key known only to the service provider (Thomlinson, "Master Key" column 9 lines 21-22), encrypting a second key using the first key and an encryption algorithm requiring a one-time password (Thomlinson,

second key viewed as the "item key" column 9 lines 20-29), and the second key being used for accessing data (Thomlinson, "item key", column 10 lines 15-16). Applicant has argued that the second key of the present invention is not used to encrypt stored items; rather it is stored at the client machine. Examiner has relied upon Shi et al US Patent No 5,875,296 to teach the storing of a key at a client computer (Shi, column 8 lines 61-63) and not for the use of cookies.

5. Applicant further argues that Examiner's use of the Shi patent to teach the storing of keys at the client is without merit. Applicant argues that cookies are not the same as or suggestive of an encrypted second key which is encrypted using a first key known only to the content provider and that cookies are a non-unique, non-encrypted, fully accessible set of data. Examiner calls attention to the specification wherein Applicant discloses, "an encrypted opaque cookie is stored on the client's machine for future accesses" (Specification "Summary of the Invention" Page 4 lines 7-8). The specification thus suggests that a cookie is a method of storing encrypted data on a client machine. Examiner has relied upon Shi's teaching of cookies only to teach the storing of an encrypted piece of data on a client machine. Examiner contends that combining Thomlinson with Shi would thus teach all the limitations of claims 1, 12, and 15.

6. With regards to the rejection of claims 9-11, 14, and 17, Applicant argues that Jablon US Patent No. 6,226,383 fails to teach or suggest the particular code generation scheme that is taught and claimed. Examiner contends that Jablon with Thomlinson teach the limitations defined in the claims. Jablon teaches the transmitting of g^a and

the identity of the user of the client machine to the content provider node where a is known only to the client (Jablon, column 4 lines 66-67, column 11 lines 19-22), the generating of g^b where b is known only to the content provider (Jablon, column 5 lines 1-2), encrypting g^b with a one-time password (Jablon, column 7, lines 16-17, column 6 lines 34-37), calculating g^(ab) by the client machine using the one-time password to decrypt the encrypted g^b (Jablon, column 5 lines 5-7 and column 6 lines 34-37, Thomlinson column 10, lines 6-8), and transmitting g^(ab) to authenticate (Jablon, column 11 lines 37-39).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1, 5, 12, 13, 15 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomlinson et al US Patent No. 6,389,535 in view of Shi et al US Patent No. 5,875,296. Thomlinson teaches a system for cryptographic protection of core data secrets.

9. With regards to claims 1,12, and 15, Thomlinson discloses a first key known as a master key (column 9, lines 20-29) that is used to encrypt a second key known as an item key (column 9 lines 20-29). When the user wishes to access data, the first key

(Thomlinson's master key) is used to decrypt the second key (column 10, lines 11-16) in order to access the data. Thomlinson teaches the use of asymmetric public key cryptography in which keys are kept private to the content provider (column 3, lines 55-57). Further, Thomlinson teaches an encryption method that utilizes a user-supplied password and entropy to encrypt keys (column 9, lines 54-56). Thomlinson lacks a reference to the storing of the encrypted second key on a client machine. Shi discloses a distributed file system web server that performs user authentication with cookies. Shi discloses a key that is stored on a client machine as a cookie (column 8, lines 61-63). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Shi's method of storing the second key on a client machine because it offers the advantage of making it unnecessary to have to enter a username/password combination each time a login is attempted (Shi, column 9, lines 10-13). The cookie containing the key could be passed to the server upon each access (column 9, lines 3-4). Further, it would have been obvious to one of ordinary skill in the art to use Thomlinson's encryption method that utilized a password and entropy on the second key because if a password change was desired it would provide a simple method: only the second key would need to be re-encrypted (column 10, lines 17-23).

10. With regards to claims 5, 13 and 16, Thomlinson and Shi disclose encryption methods as described above. Thomlinson teaches a second key termed an item key that is encrypted using an algorithm that requires a user-supplied password with an optional addition of a one-time entropy from the user application (column 9, lines 51-57

and lines 20-29). Further, Thomlinson discloses that accessing the data involves decryption that requires a user provided password as input (column 10, lines 7-8). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to apply this encryption method to the second key for reasons aforementioned. Further, it would have been obvious to a person of ordinary skill in the art to require a password to be provided in order to decrypt the data to help prevent an unauthorized user from accessing data by fraudulently using an authorized client machine.

11. Claims 2 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomlinson et al US Patent No. 6,389,535 in view of Shi et al US Patent No. 5,875,296 as applied to claims 1 and 5 above, and further in view of Danneels US Patent No. 6,571,339. Thomlinson and Shi, as described above, lack a reference to the transmitting of the identity of the client machine for use in authenticating and controlling access to data. Danneels discloses the use of a processor identification number for authentication in which a computer provides its unique processor identification number across a network as a part of the authentication procedure (column 3, lines 56-60). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Danneel's unique processor identification method because it would help provide a secure method of authentication that would prevent content from being distributed to unauthorized individuals (column 5, lines 34-39).

12. Claims 3 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomlinson et al US Patent No. 6,389,535 in view of Shi et al US Patent No. 5,875,296

as applied to claims 1 and 5 above, and further in view of Buck et al US Patent No. 6,078,866. Thomlinson and Shi, as described above, lack a reference to a one-time password being a unique user identifier that is transferred out of band. Buck discloses a system where new users create an account and are emailed a user password (column 6, lines 52-56). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Buck's method of emailing passwords because it would permit the prompt distribution of a password and allow a user to quickly begin accessing a content provider (column 7, lines 33-35).

13. Claims 4 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomlinson et al US Patent No. 6,389,535 in view of Shi et al US Patent No. 5,875,296 as applied to claims 1 and 5 above, and further in view of IBM Technical Disclosure NN9503245 (March 1, 1995). Thomlinson and Shi, as described above, lack a reference to a session key. The aforementioned IBM Technical Disclosure describes a session key, Ka, created using password substitution, a permanent key, and a random nonce (Page 1, paragraph 2). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize session keys because the use of session keys helps prevent key exposure (Page 3, paragraph 1).

14. Claims 9-11, 14, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jablon US Patent No. 6,226,383 in view of Thomlinson et al US Patent No. 6,389,535. Jablon describes cryptographic methods for remote authentication.

15. With regards to claims 9, 14, and 17, Jablon discloses two systems that exchange the keys g^a and g^b. The client machine provides an identifier to the content provider (column 11, lines 19-22). G, A, and B are randomly generated numbers and G is known to both systems (column 4, lines 55-67 and column 5, lines 1-7). B is generated and known only to one system and A is generated and known only to the other system. The value g^{a*b} is calculated in order to find a shared key K (column 5, lines 5-7). Jablon then teaches a modified version of the aforementioned key exchange where one of the exponents, termed C, is based upon a password (column 7, lines 16-17). In this modified version, the client proves knowledge of the key g^{a*b} to the server in order to prove that the client had knowledge of the password (column 7, lines 26-28). Jablon lacks a reference to the decryption of g^b using the password. Thomlinson discloses decrypting a key using a password (column 10, lines 6-8). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use passwords to decrypt keys to help prevent an unauthorized user from accessing data by fraudulently using an authorized client machine.

16. With regards to claim 10, Jablon discloses that the client sends an identifier such as a name, ID, or address to the content provider. Jablon lacks a reference to requiring that a specific user only gain access through a specific client machine. At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to require a match between a user name or ID with that of an address to provide a greater level of security by ensuring specific machines are only used by a trusted entity.

17. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jablon US Patent No. 6,226,383 in view of Thomlinson et al US Patent No. 6,389,535 as applied to claim 9 above, and further in view of Schneier Applied Cryptography. Jablon and Thomlinson as described above, lack a reference to a MAC authentication procedure. Schneier describes the one-way hash function termed a MAC that is used to verify authenticity (Page 455, Section 18.14). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Schneier's MAC authentication on g^{a*b} to authenticate the server to the client because it provides a verification method that is reliant on having the same key. Both client and server generate the same key during the authentication procedure so the MAC authentication would be an easy way to check authenticity without needing security since it is a one-way function (Page 455, Section 18.14).

Conclusion

18. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L Nalven whose telephone number is 703 305 8407. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 703 308 4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven
ALN
***

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137